PTO/SB/21 (07-06)
Approved for use through 09/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

AF

OIPE IAP97 FEB 05 2007 PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 82

Application Number	10/067,319
Filing Date	February 7, 2002
First Named Inventor	Swati Deshmukh
Art Unit	2141
Examiner Name	Quang N. Nguyen
Attorney Docket Number	19903.0016

ENCLOSURES ***(check all that apply)***

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request (1 month)
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below)*:
  1. Response to Notice of Non-Compliant Appeal Brief (in triplicate)
  2. Amended Appeal Brief (in triplicate)

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm	Bingham McCutchen LLP 3000 K Street, N.W., Suite 300 Washington, D.C. 20007		
Signature			
Printed Name	Chadwick A. Jackson		
Date	February 5, 2007	Reg. No.	46,495

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

OIPE
FEB 05 2007
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Swati Deshmukh Docket No.: 19903.0016

Application No.: 10/067,319 TC/A.U.: 2141

Filed: February 7, 2002 Examiner: Quang N. Nguyen

Title: SYSTEM AND METHOD FOR REAL-TIME TRIGGERED EVENT UPLOAD

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

In response to the Notice of Non-Compliant Appeal Brief mailed January 8, 2007, Applicant submits the following amended brief. In particular, this submission attempts to remedy the deficiencies noted by the Patent Appeals Specialist with regard to the summary of the claimed subject matter and, specifically, the identification and mapping of each independent claim (*i.e.*, claims 1, 17 and 33) to the specification by page and line number and to the drawings (if any). Other than providing this supplemental summary information in compliance with 37 C.F.R. § 41.37(c)(1)(v), the remaining portions of the brief are the same as the Appeal Brief previously submitted on November 29, 2006.

No fees are believed to be due for this submission. Should any fee be required, however, please charge such fee to Bingham McCutchen LLP Deposit Account No. 195127, Order No. 19903.0016.

Respectfully submitted,

Dated: February 5, 2007 By:

Chadwick A. Jackson, Registration No. 46,495
BINGHAM MCCUTCHEN LLP
3000 K Street, NW, Suite 300
Washington, D.C. 20007
(202) 373-6661 Telephone
(202) 295-8478 Facsimile

OIPE
FEB 05 2007
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Swati Deshmukh Docket No.: 19903.0016

Application No.: 10/067,319 TC/A.U.: 2141

Filed: February 7, 2002 Examiner: Quang N. Nguyen

Title: SYSTEM AND METHOD FOR REAL-TIME TRIGGERED EVENT UPLOAD

AMENDED APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This appeal is from the Office Action mailed August 1, 2006 finally rejecting all of the pending claims. A Notice of Appeal was timely filed on September 29, 2006. This Appeal Brief is being filed under the provisions of 37 CFR § 41.31 *et seq.*

TABLE OF CONTENTS

Table of Contents 2

Real Party in Interest 3

Related Appeals and Interferences 4

Status of Claims 5

Status of Amendments 6

Summary of Claimed Subject Matter 7

Grounds of Rejection to Be Reviewed on Appeal 10

Argument 11

Rejection under 35 U.S.C. 103 .....

Claims Appendix 13

Evidence Appendix 22

Related Proceedings Appendix 23

Conclusion 24

REAL PARTY IN INTEREST

Networks Associates Technology, Inc. is the current assignee of the present patent application. Networks Associates Technology, Inc. has been merged into McAfee, Inc., which has a business address of 3965 Freedom Circle, Santa Clara California 95054.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1, 16, 17, 32, 33, and 48-81 are pending, and claims 2-15, 18-31, and 34-47 are canceled. Claims 1, 16, 17, 32, 33, and 48-81 were rejected in the final Office Action dated August 1, 2006. The Appellant appeals the final rejection of claims 1, 16, 17, 32, 33, and 48-81.

STATUS OF AMENDMENTS

No amendments were filed subsequent to final rejection. All amendments filed by the Appellant have been duly entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to protecting computer users from Web sites hosting computer viruses and for protecting Web hosting systems from hosting Web pages that contains links to computer viruses. A System 100 includes a plurality of user systems 102A-N, such as personal computer systems or workstations operated by users, which are communicatively connected to a data communications network 104, such as a public data communications network, for example, the Internet, or a private data communications network, for example, a private intranet. *See, e.g.,* Written Description at Page 7, lines 12-17. Each user system, such as user system 102A, includes a malware agent 114 and malware scanner 116. *See, e.g.,* Written Description at Page 8, lines 8-9.

For example, according to claims 1, 17, and 33, Malware scanner 116 includes software that can detect and remove viruses and other malwares that may be present in user system 102A. *See, e.g.,* Written Description at Page 8, lines 9-11. Such software is generically known as anti-virus software or programs. If a virus or other malware is found by the malware scanner, malware scanner 116 can use the malware removal routines to respond by performing actions such as terminating processes, quarantining files, cleaning files, deleting files, etc. *See, e.g.,* Written Description at Page 20, lines 5-8. In order to detect a virus or other malicious program, an anti-virus program, such as malware scanner 116, typically scans files, processes, and/or data, which may be present in user system 102A, and/or data that is being transferred or downloaded to user system 102A, and compares the data being scanned with profiles that identify various kinds of malware. *See, e.g.,* Written Description at Page 8, line 12-16..

Malware scanner 116 typically uses one or more such malware profiles. *See, e.g.,* Written Description at Page 13, lines2. Event notification routines 226 log and transmit information relating to events generated by malware scanner 116. *See, e.g.,* Written Description at Page 13, lines 8-9. Event trigger thresholds are set for the malware agents that are present in the user systems 102A-N. *See, e.g.,* Written Description at Page 18, lines 1-2 and Table A. The event trigger thresholds are set at management server 110 in malware management program 112. The specified event trigger thresholds are then distributed to the malware agents in the user systems along with other specified policy settings. *See, e.g.,* Written Description at Page 18, lines 5-7. For example, the event trigger threshold may be set at level 2 - Minor, which means that any event with a severity level equal to or greater than 2 will trigger an immediate upload of events. *See, e.g.,* Written Description at Page 19, lines 3-5. Malware events are examined by malware agent 114 to determine their level. *See, e.g.,* Written Description at Page 20, lines 18-19. For example, if the event is a missing log file, then, if the multi-level event trigger threshold scheme shown in Table A is used, the event would be determined to be a level 2 event. If the level of the malware event is greater than or equal to the event trigger threshold that has been set for malware agent 114 a notification of the occurrence of the event is transmitted in real-time to malware management program 112. *See, e.g.,* Written Description at Page 21, lines 5-8. Once malware management program 112 receives the notification of the occurrence of the event, optional step 416 may be performed, in which malware management program 112 may transmit an alert indicating the occurrence of the event. The event alert would be sent to the administrator of the computer system and/or network via

a real-time or at least prompt communication media. Written Description at Page 21, lines 9-13.

The anti-virus program may then take corrective action, such as notifying a user or administrator of the computer system of the virus, isolating the file or data, deleting the file or data, etc. Malware agent 114 is a management agent program that provides the capability to remotely operate and manage an anti-virus program, such as malware scanner 116 as an agent on behalf of, and in communication with, malware management program 112. *See, e.g.,* Written Description at Page 8, line 19 to Page 9, line 2. Malware management program 112 provides centralized, network-wide management, administration, data collection, and reporting of malware detection and removal. *See, e.g.,* Written Description at Page 9, lines 3-5. Malware management program 112 communicates with malware agents present in the user systems, provides policies that control the operation of the malware agents, and receives event notification information from the malware agents. *See, e.g.,* Written Description at Page 9, lines 5-8.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The ground of rejection to be reviewed on appeal is:

1. Whether claims 1, 2, 9, 15-34, 48, and 50 are unpatentable under 35 U.S.C. 103 over U.S. Patent Application Publication. 2003/0131256 to Ackroyd (Ackroyd) modified by U.S. Patent No. 6,493,755 to Hansen *et al.* (Hansen).

ARGUMENT

Rejection under 35 U.S.C. 103(a)

The Examiner has rejected Claims 1, 16-17, 32-33 and 48-81 under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (U.S. Patent Application No. 2003/0131256), in view of Hansen et al. (U.S. Patent No. 6,493,755). Applicant respectfully disagrees with such rejection. Applicant respectfully submits that even if Ackroyd and Hansen were combined as suggested by the Examiner, the result would not be the present invention, as claimed.

Ackroyd discloses a managing computer within a computer network that logs messages received from individual computers within that computer network indicating detection of malware. The managing computer detects patterns of malware detection across the network as a whole a triggers associated predetermined anti-malware actions. These may include forcing specific computers to update their malware definition data, forcing particular computers to change their security settings and isolating individual portions of the computer network. However, Ackroyd does not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

Hansen discloses a network management application that provides notification of events on network devices using prepopulated notification rules. The notification rule is prepopulated by the network management application using conditions that represent the present state of the device being monitored. An associated notification action is executed when an event on a network device satisfies the conditions of the prepopulated notification rule. However, Hansen does not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

Thus, even if Ackroyd and Hansen were combined as suggested by the Examiner, the resulting combination of Ackroyd and Hansen still would not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are

received in real-time so as to prevent network congestion that adversely affects the usability of the network, as required by the present invention, for example according to claims 1, 17, and 33.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

CLAIMS APPENDIX

1. A method of reporting malware events comprising the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

16. The method of claim 1, wherein the method further comprises the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

17. A system for reporting malware events comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

32. The system of claim 17, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

33. A computer program product for reporting malware events, comprising:

a computer readable storage medium;

computer program instructions, recorded on the computer readable storage medium, executable by a processor, for performing the steps of

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

48. The computer program product of claim 33, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

49. The method of claim 1, wherein the event trigger threshold is set at a management server in a malware management program.

50. The method of claim 49, wherein the event trigger threshold is set by setting policies in the malware management program.

51. The method of claim 1, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

52. The method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

53. The method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

54. The method of claim 1, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

55. The method of claim 54, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

56. The method of claim 54, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

57. The method of claim 54, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

58. The method of claim 54, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

59. The method of claim 54, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

60. The system of claim 17, wherein the event trigger threshold is set at a management server in a malware management program.

61. The system of claim 60, wherein the event trigger threshold is set by setting policies in the malware management program.

62. The system of claim 17, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

63. The system of claim 17, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

64. The system of claim 17, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

65. The system of claim 17, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

66. The system of claim 65, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

67. The system of claim 65, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

68. The system of claim 65, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

69. The system of claim 65, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

70. The system of claim 65, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

71. The computer program product of claim 33, wherein the event trigger threshold is set at a management server in a malware management program.

72. The computer program product of claim 71, wherein the event trigger threshold is set by setting policies in the malware management program.

73. The computer program product of claim 33, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

74. The computer program product of claim 33, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

75. The computer program product of claim 33, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

76. The computer program product of claim 33, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

77. The computer program product of claim 76, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

78. The computer program product of claim 76, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

79. The computer program product of claim 76, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

80. The computer program product of claim 76, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

81. The computer program product of claim 76, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

EVIDENCE APPENDIX

None.

RELATED PROCEEDING APPENDIX

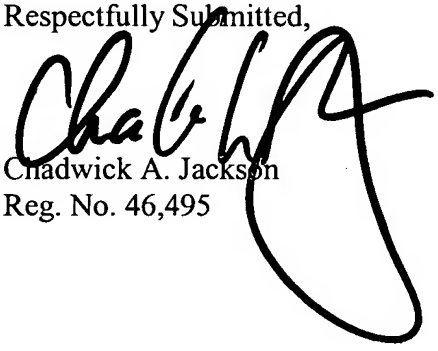
None.

CONCLUSION

In view of the foregoing arguments, the Appellant respectfully requests reconsideration and withdrawal of the claim rejections, and that the application be passed to issuance. Failing that, the Appellant respectfully requests the Board to overrule the Examiner's rejections, based on the explanations presented above, and to pass this application to issuance.

The Commissioner is hereby authorized to charge the appeal brief fee set forth in 37 CFR 41.20(b)(2) and any insufficiency or credit any overpayment associated with this application to Bingham McCutchen LLP Deposit Account No. 19-5127 (order no. 19903.0016).

Respectfully Submitted,



Dated: February 5, 2007

Chadwick A. Jackson
Reg. No. 46,495

Bingham McCutchen LLP
3000 K Street, NW
Suite 300
Washington, DC 20007
(202) 373-6029